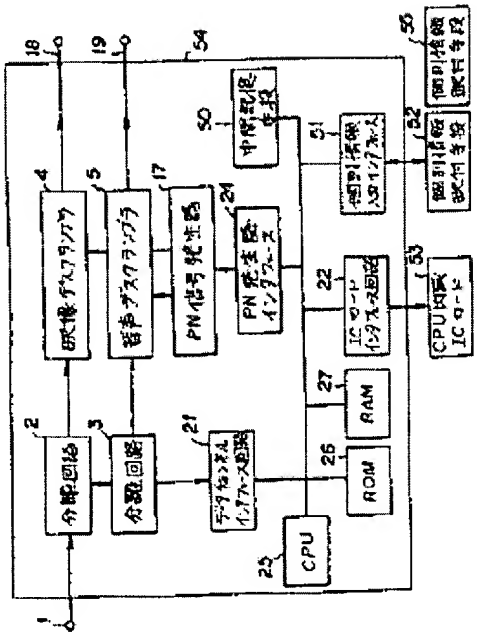
BROADCAST RECEPTION CONTROL SYSTEM

Publication number: JP4150333
Publication date: 1992-05-22
Inventor: NANBA SEIICHI; KIMURA TAKESHI
Applicant: JAPAN BROADCASTING CORP
Classification:
- International: ***H04K1/04; H04H1/00; H04L9/10; H04L9/20; H04N7/167;*** **H04K1/04; H04H1/00; H04L9/10; H04L9/18; H04N7/167;** (IPC1-7): H04K1/04; H04N7/167
- European:
Application number: JP19900270575 19901011
Priority number(s): JP19900270575 19901011

Abstract of **JP4150333**

PURPOSE:To attain safety and ease of management of secret information by including a processing having secret information such as ciphering deciphering processing of relating information into a removable security module such as an IC card with a CPU built therein. CONSTITUTION:When a service contract is placed with a broadcast enterprise, an IC card 53 into which a CPU is built in having service individual information (content of contract and work key KW) is given to the user. When the card 53 is loaded to a paid decoder main body 54, the processing is implemented via an IC card interface 22, program information is given to the card 53 and a decoded Ks is outputted to a PN generator 17. When the contract is revised, the user receives an individual information distribution means 52 including new individual information. The individual information included therein is once stored in an intermediate storage means 50 via an individual information input interface 51 and transferred to a card 53 via the interface 22. The preceding individual information on the card 53 is rewritten, not required, and when available, the transferred individual information is added to the old information.



⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−150333

⑤1Int. Cl.[5]	識別記号	庁内整理番号	⑬公開　平成4年(1992)5月22日
H 04 K 1/04		7117−5K	
H 04 N 7/167		8324−5C	

審査請求　未請求　請求項の数 3 (全15頁)

⑤4発明の名称　放送受信制御方式

⑳特　願　平2−270575
㉒出　願　平2(1990)10月11日

⑦2発明者　難波　誠一　東京都世田谷区砧1丁目10番11号　日本放送協会放送技術研究所内
⑦2発明者　木村　武史　東京都世田谷区砧1丁目10番11号　日本放送協会放送技術研究所内
⑦1出願人　日本放送協会　東京都渋谷区神南2丁目2番1号
⑦4代理人　弁理士　谷　義一　外1名

明　細　書

1．発明の名称

放送受信制御方式

2．特許請求の範囲

1）スクランブルされた放送信号と、当該放送信号とともに送られる前記スクランブルされた放送信号をデスクランブルするための暗号化された情報と、別途送られる少なくとも前記暗号化された情報を復号するための鍵情報とを受け取り、
前記鍵情報により前記暗号化された情報を処理して前記スクランブルされた放送信号をデスクランブルする放送受信方式において、
前記暗号化された情報を処理すると共に、前記鍵情報を記憶しうる取り外し可能なセキュリティモジュールと、
内容の異なる前記鍵情報を含む媒体と
を別個に設けることを特徴とする放送受信制御方式。

2）前記鍵情報を含む媒体の内容を前記取り外し可能なセキュリティモジュールに転送して、前記暗号化された情報を処理することを特徴とする請求項第1項に記載の放送受信制御方式。

3）前記鍵情報を含む媒体と前記取り外し可能なセキュリティモジュールが同一の電気的，機械的インタフェースを有することを特徴とする請求項第1項もしくは第2項のいずれかに記載の放送受信制御方式。

(以下余白)

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、有料放送方式において、複数の放送事業者が独自の課金方式等の営業形態をとることができ、安全性が高く、秘密情報や鍵の管理の問題を解決し、かつ受信者の操作の容易な受信制御方式を与えるものである。

〔発明の概要〕

本発明は、放送された信号が例えば受信の契約を行った人のみが受信できるようにするために、信号をスクランブルして放送し、契約した人にはそれを復元するための鍵情報を送ることによって受信できるようにする有料放送方式において、複数の放送事業者が独自の課金方式等の営業形態をとることができ、安全性が高く、放送事業者や受信機製造業者の間での秘密情報や鍵の管理の問題を解決し、かつ受信者の操作の容易な受信制御方式を与えるものである。

このような受信制御方式は、受信機での秘密の

いずれの有料方式にも適用可能なものである。

〔従来の技術〕

有料放送方式においては、契約者のみが放送を視聴できるようにするために、放送信号をスクランブルして放送し、契約者にはこのスクランブルを元に戻す（デスクランブル）ための鍵を別途配布して復元を行う。信号をスクランブルする方法としては種々あり、本発明とは直接関係しないが、例えば、放送衛星によるテレビ放送や高精細テレビジョン（ハイビジョン）放送では、映像信号については画面を横方向に乱すラインローテーション方式（走査線内信号切替方式）や縦方向に乱すラインパーミュテーション方式（走査線転移方式），音声信号についてはディジタル化された信号に擬似ランダム信号（以下PN信号という）系列を加算する方式が用いられる。

このスクランブルの方法は長時間固定しておくと信号を詳細に観測することにより解読されることがあるので、比較的短時間（例えば1秒程度）

暗号アルゴリズムや鍵に基づく処理の部分に取り外し可能なセキュリティモジュール、例えばCPU内蔵のICカードを用いると実現できるが、その中に含まれる比較的短時間で更新される鍵情報（例えば月ごとに変わる鍵）や各人の契約内容を配布するためにICカードを交換したり内容を書き替えたりすると、運用コストが高くなるという問題も残されていた。

本発明はこの問題も解決できる受信制御方式を与えるもので、CPU内蔵のICカード等の取り外し可能なセキュリティモジュールと、短時間で更新する秘密情報を配布する媒体とを別個としたものである。

この方式を用いることにより、秘密情報の管理という本質的な部分には安全性が高く管理の容易な方式を採用でき、日常の運用の面ではコストの低い媒体を用いることができるという非常に有効な有料放送の受信制御方式を実現することができる。なお、本方式はテレビジョン，ハイビジョン（高精細度テレビジョン），各種データ放送等の

に変化させることが必要である。この変化はスクランブル鍵（以下K_sと略記する）で制御され、この情報がデスクランブラへ伝えられる。送信側と受信側ではこのK_sを基に同一のPN信号を発生させ、放送信号のスクランブル及びデスクランブルを行う。

上記K_sは放送信号を実時間で制御する必要があるので、通常は放送信号と同じ伝送路で送られる。従って、第三者にも容易に知られることとなるので、別な鍵で暗号化して送られる。この鍵はワーク鍵（以下K_wと略記する）と呼ばれる。このK_wも固定しておくと破られることがあるので、例えば1ヶ月や1年などの間隔で変更することが必要である。K_wを受信機へ伝える媒体としては放送信号と同じ伝送路（電波など）もしくはICカード，磁気カード等の物理媒体，電話線などの有線媒体が用いられる。

ここで、特に電波など第3者がアクセスしやすい伝送路で送る場合は、契約者ごとに個有のマスタ鍵（以下K_mと略記する）で暗号化して伝送され

る。

以上のようなシステム構成の場合、契約者以外にはK_wを渡さないことにより受信を制御することができる。なお、上記各種の鍵や、放送中の番組が各受信者の契約内容と合致しているかを受信機で判定してデスクランブルを行うための情報を総称して関連情報と呼ぶ。この中には、鍵K_sと放送中の番組の属性を示す情報等とによる「番組情報」，特定の受信機のデスクランブル機能を放送波により停止させたり、再起動させたりするための「制御情報」，鍵K_wと各受信者の契約内容を表わす情報等による「個別情報」などの種類がある。ここで、「番組情報」と「制御情報」は鍵K_wで暗号化され、外からは区別できない形にして送信される。

これらの関連情報を放送波で送る場合には、例えば、衛星放送のテレビ放送やハイビジョン放送では、データチャンネルでパケット伝送される。

さらに、各種のディジタル信号を送ってサービスを行うデータ放送も開発されている。データ放送では、文字信号，ファクシミリ信号，各種ソフトウェア，コード化した音楽演奏情報，その他各種のデータ信号を送ってサービスを行う。この場合、各信号に適したスクランブル方式が異なることも考えられ、また営業形態も異なると想定されるので有料方式は統一するのが適当でない場合も考えられる。しかし、受信機や受信者の操作は出来る限り統一されることが望ましい。

ここで、各種データ放送サービスの信号はパケットの形に統一して送信される（前記テレビ放送の有料方式の関連情報のパケットと同じ構成である）。有料放送を行う場合には、このデータ放送信号のパケットの一部がスクランブル（暗号化）され、これを復元するための関連情報がデータ信号の送信の前に予め送られるのが一般的である。

各放送事業者が有料放送を行う場合には、種々の料金設定方式のうちから特定の方式を採用し、それに基づいて受信者との契約を行う。この契約

内容（例えば料金設定方式としてフラットフィー方式を用いる場合は契約期限など，ティア方式を用いる場合では契約期限と契約ティアなど、ペイパービュー方式を用いる場合では前払い金など）と前記ワーク鍵K_wを受信機の有料デコーダに送る。

放送を受信するときには、その放送が契約内容と合致しているか否かを有料デコーダ内で判定し、ペイパービュー方式では残金があり視聴希望の入力がなされたことを確認し、これらの条件が満足されたときにデスクランブルを行い番組の視聴が可能になる。

上記契約内容とK_wを受信機の有料デコーダに送る方法として放送波を用いる場合には、有料デコーダ内に不揮発性のメモリを持ち、当該有料デコーダと同じID番号を持つ個別情報が送られたときに、その暗号を自分のマスタ鍵K_mで復号して、その情報を不揮発性のメモリに書き込む。

この場合、情報を送るときに契約者の受信機の電源が入っていなければならないこと，大量の情報が集中すると伝送に時間遅れを生じること（情報伝送に使用する伝送路の容量によるが、1000万件程度が集中すると１日のオーダの遅れ），確実に送るために何回かの再送が必要であることなど管理運用面で問題を生じる可能性がある。

ICカード等のカードを用いて個別情報を配布する場合には、契約内容とK_wを書き込んだカードを郵送するか、特定の端末で発行することになる。このとき、外部から読み出し可能な媒体ではK_mで暗号化する必要がある。

有料デコーダで関連情報を処理する部分はCPUを内蔵した集積回路で構成されるが、暗号アルゴリズムや各種の鍵情報が外部から読み出せないことが必要である。この集積回路を有料デコーダ内部に埋め込む方式とすると、外部とのインタフェース部分が不要となり有料デコーダ本体のコストが下げられるので、利用されることが多い。しかし、暗号アルゴリズムや鍵のうちK_mなどの秘密情報が有料デコーダの内部に埋め込まれるので、有料デコーダの製造や、個別情報の配布を放

送事業者側で管理する必要がある。このとき、放送事業者が複数になる場合、受信者側では同一の有料デコーダで受信できることが必要になるので、放送事業者間で秘密情報の共通管理が必要となる。

このような問題を解決するため、有料方式の関連情報を処理する集積回路の部分をCPU 内蔵のICカード等に含め、これを有料デコーダ本体から取り外し可能な形態すなわち取り外し可能なセキュリティモジュールとすることが検討されている。有料デコーダ本体にはICカードのリーダライタ部分が追加されるが（これは単なる接点で良い）、秘密に管理する部分がなくなるので、大量生産が容易となり、また店頭で自由に販売することができ、製造・流通の両面でコストの軽減が図れる大きな利点が得られる。

放送事業者はそれぞれの営業形態による処理プログラムを内蔵したICカードを発行することができ、事業者間で秘密情報を共通管理する必要もなくすことができる。また、万一暗号アルゴリズムが破られた場合にも、ICカードに内蔵されている暗号アルゴリズムを変更したICカードを契約更新時に発行することにより、容易に対策することができる。

また、データ放送の受信機の一部としてCPU 内蔵のICカードを用いる場合には、サービスごとの有料放送の受信のための処理が行えるばかりでなく、ICカードの処理速度が満たされればデータ信号のデスクランブル処理もICカードの内部で行うことも可能となる。

次に、図面を参照して従来技術を詳細に説明する。

第７図は従来のテレビジョンやハイビジョンの有料放送受信機の機能ブロック構成例を示している。スクランブルされた放送信号１から分離回路２，３でそれぞれスクランブルされた映像信号，スクランブルされた音声信号が分離され、映像デスクランブラ４，音声デスクランブラ５に加えられる。同時に分離回路３でデータチャンネルの関連情報が分離され、番組情報６が復号回路８に，

個別情報７が復号回路９に加えられる。

まず、個別情報７は復号回路９で各有料デコーダに個有のマスタ鍵K_m10で暗号復号され、ワーク鍵K_w11と各受信者の契約内容に関する情報12が得られる。番組情報６は放送番組に付随して頻繁に送られ、復号回路８でワーク鍵K_w11により暗号復号が行われ、スクランブル鍵K_s13と放送番組の属性に関する情報14が得られる。

契約条件比較回路15で受信中の放送番組の属性14が契約内容に関する情報12に合致しているかを比較し、条件が合致する場合はK_s出力制御回路16を制御してK_sをPN信号発生器17に出力する。合致しない場合は、通常は全て０のK_sがPN信号発生器17に出力される。

PN信号発生器17で発生したPN信号で、映像信号と音声信号のデスクランブルを行い、復元された映像信号18と音声信号19が得られる。

以上は電波アドレッシングで個別情報を配布する場合の機能構成であるが、個別情報をICカード等で配布する場合は、ICカード等の入力インタフェース20が付加され、その出力の個別情報が復号回路９へ加えられる。

なお、復号回路の８と９は分離して示してあるが、暗号アルゴリズムが同一である場合には共用するのが一般的である。

また、これらの機能は図には直接示していないCPU によるプログラムで実行されるのが一般的である。

上述の構成は関連情報の処理部分が有料デコーダ内に埋め込まれている場合にも共通であるが、CPU 内蔵のICカードとして取り外し可能な形態とする場合は例えば図の点線部分がICカードの中に含まれる。

ただし、この切り分けはICカードの構造や性能により流動的であり、将来、種々の形態が利用されることも考えられる。

なお、ICカードの場合は個別情報はICカード内に予め記録して配布するので、入力インタフェース20は含まれない。

ICカードを用いる場合の有料デコーダ本体とIC

カードをインタフェースする回路構成例を第８図に示す。信号のデスクランブラ部分は第７図と同一であるので説明を省略する。分離回路３で分離されたデータチャンネルの信号はデータチャンネルインタフェース回路21を通して入力される。

ここで関連情報のパケットが選択され、ICカードインタフェース回路22を通してICカード23へ出力される。このインタフェース回路22はICカードの接点、さらに、カードセンサ，カード排出機構なども含まれる。ICカード23の内部で関連情報のうちの番組情報が、ICカード内部に記憶されている個別情報（K_w及び契約内容等）により処理された後、復元されたK_sがICカードインタフェース22を介してPN発生器インタフェース24に出力される。

なお、図に示したCPU25 は信号の流れを制御する程度の簡単な機能しか持たず、秘密情報の処理等の主要な部分は全てICカード23の内部のCPU で行う。従って、第８図のROM26 はCPU25 で行う簡単なプログラムの格納用、またRAM27 はその作業

用のメモリであり、本質的なものではない。

この構成例では、有料デコーダあるいは受信者（契約者）を識別するID情報は有料デコーダ本体28には含まれず、ICカード23の内部に含まれる。ただし、営業形態により受信者の個別管理を行わないことも可能であり、この場合にはICカード23の内部にはID情報を含めないか、あるいは全て同一のID情報を記録しておくことになる。

第９図はデータ放送の有料方式の受信機である。データ信号のデスクランブルは有料デコーダ本体30で行い、ICカード31の内部では関連情報の処理を行う場合の構成例である。入力されたデータチャンネルの信号32はデータチャンネルデコーダ33で処理され、ICカード31に記録されているサービス識別(SI)コード34がデータチャンネルインタフェース35を通して入力され希望のデータ放送サービスのパケットが分離される。

このパケットにはスクランブルされたデータ信号のパケットとデスクランブルを制御するための関連情報のパケット等が含まれているので、デー

タ分離回路36でICカード31内部に記録された情報に基づき関連情報のパケットを分離してICカードインタフェース38を通してICカード31に入力される。

ICカード内で関連情報が処理された後デスクランブル鍵K_s40がPN発生器インタフェース39を通じてPN信号発生器41に加えられる。このPN信号発生器の出力のPN信号系列によりデータ信号デスクランブラ42でデスクランブルが行われ、デスクランブルされたデータ信号43が得られ、各種データサービスのデコーダへ出力される。

ここで、デスクランブル鍵K_s40はPN信号発生器に与える初期値やPN信号発生器の構造データ等で構成される。

なお、第９図において、有料デコーダ本体30内部の信号デスクランブラはPN信号系列の加算によるいわゆるストリームサイファー方式によるのが一般的であるが、これに限られるものではない。また、図中のCPU44，ROM45，RAM46は第８図の説明で述べたように特に重要な意味を持つものではない。

第10図は、データ放送の有料方式の受信機でデータ信号のデスクランブルもICカード48の内部で行う場合の構成例である。データチャンネルデコーダ33で分離された希望のデータ放送サービスのパケットはICカード48へ送られる。ICカード48の内部では、まず関連情報が処理されデスクランブル鍵K_sが得られ、これに基づいて続いて受信されるスクランブルされたデータ信号のデスクランブルが行われ、その結果の復元されたデータ信号43が出力インタフェース49を通して出力される。

〔発明が解決しようとする課題〕

ところで、有料放送の受信機における関連情報の処理部分をCPU 内蔵のICカードで行う場合には、受信機への個別情報の配布もICカードで行うのが基本である。このとき、ICカードの中には、各加入者の契約内容とK_wと、関連情報の処理プログラムが含まれることになる。契約を更新する場

合には、契約内容とKwの部分が書き替えられたカードが発行される。この方法としては、新たなカードを新規に発行して配布する，前のカードに対して放送事業者側の特定の装置で、契約内容とKwの部分を書き替えるなどがある。

勿論、放送波で個別情報を各有料デコーダに配布する（これを電波アドレッシングと呼ぶ）場合の有料デコーダに埋め込まれた集積回路の処理プログラムをICカードに内蔵すれば、ICカードを用いる方式で電波アドレッシング方式を実施することができる。この方式は、離島等でICカードによる配布が容易でない場合には必要であるが、通常では前述のように個別情報が送られるときには、受信機の電源を入れ、そのチャンネルに同調していなければならないという問題が解決されないので、用途は限定される（機能としては必要である）。

ところで、ICカードの発行あるいは内容の書き替えで個別情報を配布する場合に問題になる点として、複数の放送事業者の有料放送を単一の有料

放送受信機（有料デコーダ）で受信するときの取扱がある。これには、次のような方法がある。

(1) 放送事業者ごとに別なカードを用いる方式。

放送事業者ごとに独自な有料方式が採用できるので、最も融通性の高い方式である。受信者は放送事業者ごとに契約してICカードを受け取りあるいは購入して、受信するときに、希望のカードを有料デコーダに挿入する。この方式はカードの枚数が増えるので、操作の点やカードコストの点が問題となる。また、複数の放送事業者の番組を予約受信するような場合には、有料デコーダに複数のカードが挿入できる機構等が必要になる。

(2) 一枚のカードに複数の放送事業者の情報を記録する方式。

これには、同一の処理プログラムで個別情報（契約内容やKw）のみが異なる場合と、処理プログラムも個別情報の内容も異なる場合とがある。これらは、使用するICカードの記憶容量と関係するが、大容量化していく傾向であるので、技術的にはいずれも可能である。しかし、この方式は

カード発行あるいは更新の方法に問題があり、営業が同一に行われない場合には、受信者の入手手段が繁雑になる。例えば、ある事業者から入手したカードを別な事業者に持参して情報を追記してもらうなどの操作が必要になる。従って、事業者間で互いに情報を転送できる体制があり、受信者が容易にアクセスできるシステムとなっていなければ実現しにくい。

よって本発明の目的は、有料放送の関連情報をCPU 内蔵のICカードで処理して受信を制御する方式において、複数事業者の個別情報を統一的に扱え、受信者の操作や事業の運営等が簡略化される放送受信方式を提供することにある。

【課題を解決するための手段】

本発明は、スクランブルされた放送信号と、当放送信号とともに送られる前記スクランブルされた放送信号をデスクランブルするための暗号化された情報と、別途送られる少なくとも前記暗号化された情報を復号するための鍵情報とを受け取

り、前記鍵情報により前記暗号化された情報を処理して前記スクランブルされた放送信号をデスクランブルする放送受信方式において、前記暗号化された情報を処理すると共に、前記鍵情報を記憶しうる取り外し可能なセキュリティモジュールと、内容の異なる前記鍵情報を含む媒体とを別個に設けることを特徴とするものである。

【実施例】

次に、本発明の第１の実施例を第１図に示す。これは、第８図に個別情報の中間記憶手段50と個別情報入力インタフェース51，個別情報配布手段52を追加した構成である。（従って、他のものは共通の番号としてある）。この装置を用いた場合の動作例は次のようになる。

ある放送事業者とあるサービスの受信の契約を行うと、当該放送事業者，当該サービスの個別情報（契約内容とワーク鍵Kw）を含んだCPU 内蔵のICカード53が渡される。このICカードを有料デコーダ本体54のリーダ部に挿入すると、ICカード

インタフェース22を介して関連情報の処理が行われる。すなわち、番組情報がICカード53に渡され、ICカード53内で処理された後復元されたKsがPN発生器17に出力される。

次に、契約を更新するときには新たな個別情報（契約内容とKw）を含んだ個別情報配布手段52を受け取る。この個別情報配布手段52はICカードあるいは磁気カードあるいは電話線で送られる情報などいずれでも良い。この個別情報配布手段52に含まれる個別情報は、個別情報入力インタフェース51を介して個別情報の中間記憶手段50へ一旦記憶される。

ここで、個別情報入力インタフェース51は個別情報配布手段52がICカードの場合はICカードリーダ，磁気カードの場合は磁気カードリーダ、電話線で送られる情報の場合には電話線用モデムとなる。

個別情報の中間記憶手段50へ一旦記憶された個別情報は、適当な時にICカードインタフェース22を介してICカード53へ転送される。ICカード53には以前の個別情報が記憶されているので、これが不要の場合には書き替え、まだ使用可能な場合に転送された個別情報を追加する。

ここで、ICカード53内には複数すなわち例えば1放送事業者，1サービス当り今期の個別情報と来期の個別情報の2個，さらにこれの通常の視聴者が契約する事業者，サービス（同じ有料デコーダを使用するもの）数倍の個別情報が記憶できるようになっている。

さらに、この有料デコーダ54を持つ受信者が、他の放送事業者のサービスを受信する場合には、その個別情報配布手段55を入手する。その後は、前述と同様、その中の個別情報を一旦個別情報の中間記憶手段50に記憶し、最終的にICカード53に転送する。

ところで、個別情報は外部からアクセス可能な場合には暗号化する必要があり、本発明のように有料デコーダ本体内を転送される場合には暗号化する必要がある。従って、個別情報の中間記憶手段50には暗号化した個別情報が記憶され、暗号化

されたままICカード53に転送される。この暗号の復号は外部からアクセスできないICカード53の内部で行われ、復号された個別情報がICカード53の中に記憶される。

このとき、個別情報配布手段52あるいは55内の個別情報を暗号化しているアルゴリズムはICカード53の内部にある復号処理プログラムに対応している必要がある（ただし、ICカード53にはその容量によるが複数の暗号復号処理プログラムを含めることが可能である）。

また、この個別情報の暗号を復号する鍵もICカード53の中に含まれている必要があり、通常は受信者個有のマスタ鍵Kmが用いられる。

なお、第1図による本発明の実施例では、個別情報入力インタフェース51とICカードインタフェース22は別個に設けられているので、それらを適当に制御することにより、個別情報の中間記憶手段を省略することも可能である。

本発明の第2の実施例は第2図のようになる。

これは、第1図示の第1の実施例で個別情報入力インタフェース51がICカードインタフェース22と同一とした場合である。従って、前述の個別情報配布手段52,55 はICカードとなる。

ただし、このICカードはCPU を内蔵する必要はなく、接点が共通であれば、単なるメモリカードで良い。

この第2の実施例における操作手順と動作例は次の通りである。

まず、第1の実施例と同様、ある放送事業者とあるサービスの受信の契約を行うと、その個別情報を含んだCPU 内蔵のICカード53を受け取り、有料デコーダ本体54のリーダ部に挿入して受信する。契約更新時には、新たな個別情報を含んだ個別情報配布手段52（以下、ICメモリカードと記す）を得る。

有料デコーダ本体54から一度CPU 内蔵のICカード53を排出し、ICメモリカード52を挿入する。ICメモリカード52内の個別情報は、一旦個別情報の中間記憶手段50に記憶される。

次に、ICメモリカード52を有料デコーダ本体54から排出し、再びCPU 内蔵のICカード53を挿入する。第１の実施例と同様、個別情報が中間記憶手段50からICカード53内へ転送される。複数の放送事業者やサービスを受信する場合にはICメモリカード55を入手し、前と同様、一旦中間記憶手段50に記憶して、最終的にICカード53内へ転送する。

このとき、複数枚のICメモリカードの個別情報を順次中間記憶手段50に記憶したのち、全体をICカード53内へ転送するのが操作上容易であるが、この場合には中間記憶手段50に複数の個別情報が記憶できる容量を持つ必要がある。この方式はICカードのリーダ部が１個で良く、実際的である。

個別情報の中間記憶手段50の媒体としては、通常のRAM(ランダムアクセスメモリ）やEEPROM（電気的消去可能な書き替え可能なリードオンリメモリ）等が考えられる。ICメモリカードから個別情報を記憶したのちCPU 内蔵のICカードに転送するまでの間に電源を切らなければRAM で良いが、そのような点を受信者に意識させずに、ICメモリカードは適当なときに転送しておき、番組を受信するときにCPU 内蔵ICカードを挿入すると自動的に転送されるようなシステムとするには、EEPROM, 電源バックアップを行ったRAM 等を使用する必要がある。

なお、これらのメモリは、各図の中に含まれるRAM27 やROM26(書き替え可能の場合）を利用することも可能であるが、これは回路設計上の問題であり、ここでは分離したメモリで説明している。

また、個別情報の転送は、CPU25 の管理の下に行われる。

第３図および第４図は、それぞれ第９図および第10図に示したデータ放送の有料方式の受信機に本発明を適用する場合の回路構成例を示している。これらの回路の動作については、これまでに述べた内容と重複する部分が多いので、特徴的な部分について述べることとする。

２７

２８

第３図の構成はデータ信号のデスクランブルをICカードの外で行う場合であり、ICカードの中では関連情報の処理が行われる。すなわち、データチャンネルで送られたデータ放送サービスのパケットの内からデスクランブルを制御するための関連情報のパケットが分離されCPU 内蔵のICカード56に送られる。

このICカード56の中には少なくとも第５図に示すような情報が記録されている。ここで、第１の個別情報は最初の契約時に書き込まれているもので、複数の契約がなされている場合には複数の個別情報になるがここでは説明を簡単にするため１個とする。従って、第２の個別情報以下は最初は空白である。放送を受信するときには、データチャンネルから暗号化されたデスクランブル鍵K$_s$を含む番組情報がデータチャンネルから分離されICカード56の中に取り込まれる。

ICカード56の内部で関連情報処理プログラムにより第１の個別情報に含まれるK$_m$で暗号が復号され、契約内容の合致が判定された後、K$_s$が出力されPN発生器41へ出力される。

次に、契約を更新する場合には新たな個別情報を含むICカード57A(この場合はICメモリカードで良く以下ではICメモリカードと記す）を入手し、有料デコーダ本体58に挿入し（ICカード56と差し替える）情報内容を個別情報の中間記憶手段59へ一旦記憶する。さらに、別の事業者やサービスと契約する場合もそれぞれの個別情報を含むICメモリカード57B を入手し、有料デコーダ本体58へ挿入し順次情報内容を中間記憶手段59へ一旦記憶する。

最後に、再びCPU 内蔵のICカード56を挿入すると、中間記憶手段59の内容がICカード56へ転送され、第５図で第２の個別情報と記した領域以下へ順次記憶される。

なお、営業の形態によっては、第１の個別情報も最初はICカード56に含まず、ICメモリカードから転送することもありうる。この点は、第１図，第２図の実施例の場合も同様である。

放送を受信する場合は、各放送に付随して送ら

２９

３０

れる番組情報の中には復号処理に使用する個別情報を識別するコードを含めるようにするので、これに基づき復号処理を行う。

第４図の構成は、データ信号のデスクランブルをICカードの内部で行う場合であり、この場合のCPU 内蔵のICカード60は、第６図に示すように、信号デスクランブル処理プログラムが追加されている。ICカード60の内部で関連情報処理プログラムにより第１の個別情報あるいは番組情報で指定された個別情報に含まれるK_wで暗号が復号され、契約内容の合致が判定された後、K_sが得られる。

続いて、ICカード60にはデータチャンネルから当該データ放送サービスのスクランブルされたデータ信号が入力されるので、ICカード内の信号デスクランブル処理プログラムで前記K_sを用いてデスクランブルが行われる。その結果のデスクランブルされたデータ信号が出力インタフェース49を通して各サービスデコーダへ出力される。この場合、ICメモリカード61A,61B などや、中間記憶

手段63の機能や動作については第３図で説明したものと同様であるので省略する。

また、ここでは第３図および第４図の構成、すなわちテレビジョン等の有料方式の構成では第２図の構成に対応する、ICカードのリーダ部が１個の場合について説明したが、第１図の構成に対応する別個の個別情報入力インタフェースを持つ場合についてもテレビジョン等の有料方式に適用した場合と同様の機能がデータ放送の有料方式で実現できることは明らかであり、これについても説明は省略する。

ここで、本発明の有料放送の受信制御方式を複数の放送事業者で使用する場合について補足しておく。

CPU を内蔵したICカード等の取り外し可能なセキュリティモジュールを利用する有料放送の受信方式は、複数の放送事業者がサービスを行う場合、暗号アルゴリズムや鍵情報等の秘密情報を共通に管理する際の問題がなくなる利点があった。

しかし、個別情報の配布等の契約管理は独立とするが、秘密情報の管理は共通とする場合にも、放送を受信する際に別個のICカードを入手し必ず差し替えねばならないことは好ましくない。

本発明の方式は、この問題を個別情報の配布は別カードとし、受信処理は共通のカードで行うことで解決している。このとき、例えば、第１の放送事業者と第２の放送事業者とがある場合、ある受信者が最初に第１の放送事業者と契約すると、第１の事業者からCPU 内蔵のICカードを入手する。

その後、第２の事業者と契約すると、その個別情報を含んだICメモリカードの配布を受け、その内容を第１の事業者のCPU 内蔵ICカードに転送して受信することになる。

逆に、先に第２の事業者と契約した場合は、第２の事業者からCPU 内蔵のICカードを受け、後に第１の事業者の個別情報を入手して転送して受信することになる。勿論、この種の営業形態は種々考えられるので、ここで示したのはその一例である。

ここで、CPU 内蔵のICカードには複数の個別情報が記憶できる容量のメモリが必要であるが、この容量は時代とともに増やしていくことも可能であり、足りなくなれば容量の大きいカードを発行することで受信機本体には手を加えずに対応可能である。このようなことは受信機本体内にメモリが埋め込まれている場合には困難である。

ところで、複数の事業者の間で管理すべき秘密情報は関連情報の暗号化アルゴリズムと鍵情報が中心である。ただし、暗号化アリゴリズムは公開される場合もあり、この場合は鍵情報の管理が重要になる。

ここで、事業者間で問題になるのは、個別情報の暗号化を行うためのマスタ鍵$K_{m,i}$(ただしｉはデコーダIDを示す）である。これは、元来個別情報を電波で配布する電波アドレッシングを可能とする場合に不可欠なものであるが、本発明のように後に個別情報をCPU 内蔵のICカードに転送する際にも必要である。従って、CPU 内蔵のICカードに

はマスタ鍵K_mの情報が含まれており、別な事業者はこのK_mを用いて個別情報を暗号化する。

〔発明の効果〕

以上説明したとおり本発明によれば、テレビジョン放送，ハイビジョン放送，データ放送等の有料方式において、関連情報の暗号復号処理等の秘密情報を含む部分をCPU 内蔵のICカード等の取り外し可能なセキュリティモジュールに含めることにより、

① 有料方式デコーダ本体を含む受信機本体には秘密管理を必要とする部分が含まれていないので、製造，販売等が容易になる。

② ICカードの発行を独立に行うことで、放送事業者間で鍵情報等の秘密管理を行う必要がなくなる。

③ 将来、暗号方式が破られた場合にもICカードを発行し直すことで解決できる。

といった多くの利点が得られる。しかし、契約更新の度に処理プログラムを含むCPU 内蔵のICカードを発行することは無駄やICカードの内容の書き替え操作の繁雑性の問題が残っていた。

本発明によれば、契約更新時や同じ方式の個別情報を用いる放送事業者間では個別情報のみを含むICカード等の媒体を用いることができるようになり、取り外し可能なセキュリティモジュールを用いる有料放送受信制御方式の利点が強化される。ICカードを用いる場合、更新時にはCPU を内蔵しないICカード，すなわちメモリのみを含むカードを使用することができ、大幅なコストの低減が実現できる。

また、本発明の放送受信制御方式においては、契約更新時や複数の事業者と契約するときには、過渡的に複数のカードが存在するが、これらの内容は全てCPU 内蔵のICカードに転送してから使用するので、放送を受信するときには１枚のICカードだけで動作するようになる。

従って、受信するときにカードを差し替える手間がなくなる。例えば、複数の放送事業者の番組を待ち受け受信や予約録画するときの問題が解決

されるなどの利点が得られる。

４．図面の簡単な説明

第１図は本発明による受信機構成の第１の実施例を示す図、

第２図は本発明による受信機構成の第２の実施例を示す図、

第３図は本発明をデータ放送の有料方式に適用した場合の受信機構成の実施例(1) を示す図、

第４図は本発明をデータ放送の有料方式に適用した場合の受信機構成の実施例(2) を示す図、

第５図はCPU 内蔵のICカードに記録されている情報の例（信号デスクランブルをICカードの外部で行う場合）を示す図、

第６図はCPU 内蔵のICカードに記録されている情報の例（信号デスクランブルをICカードの内部で行う場合）を示す図、

第７図はテレビジョンやハイビジョンの有料放送受信機の機能ブロックの構成例を示す図、

第８図はCPU 内蔵のICカードを用いる有料放送受信機の回路構成例を示す図、

第９図はデータ放送の有料方式受信機の構成例(1)〔デスクランブル処理を有料デコーダ本体内で行う場合〕を示す図、

第10図はデータ放送の有料方式受信機の構成例(2)〔デスクランブル処理をICカード内で行う場合〕を示す図である。

１…放送信号、
２，３…分離回路、
４…映像デスクランブラ、
５…音声デスクランブラ、
17…PN信号発生器、
18…復元された映像信号、
19…復元された音声信号、
21…データチャンネルインタフェース回路、
22…ICカードインタフェース回路、
24…PN発生器インタフェース、
25…CPU 、
26…ROM 、

27…RAM 、

50…中間記憶手段、

51…個別情報入力インタフェース、

52…個別情報配布手段、

53…CPU 内蔵ICカード、

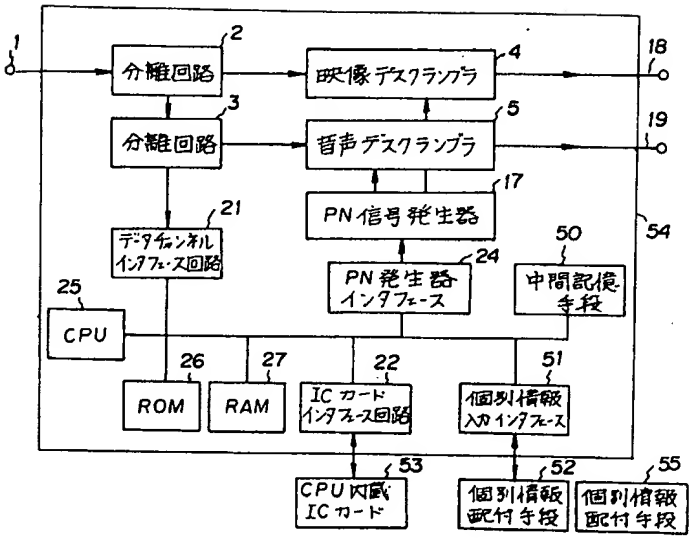
54…有料デコーダ本体、

55…個別情報配布手段。

特許出願人　　日本放送協会

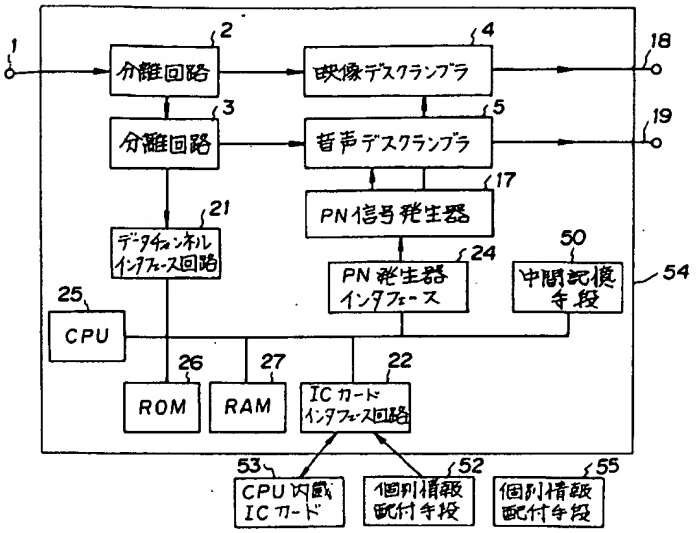
代理人　　弁理士 谷　義一
代理人弁理士 阿部和夫

39



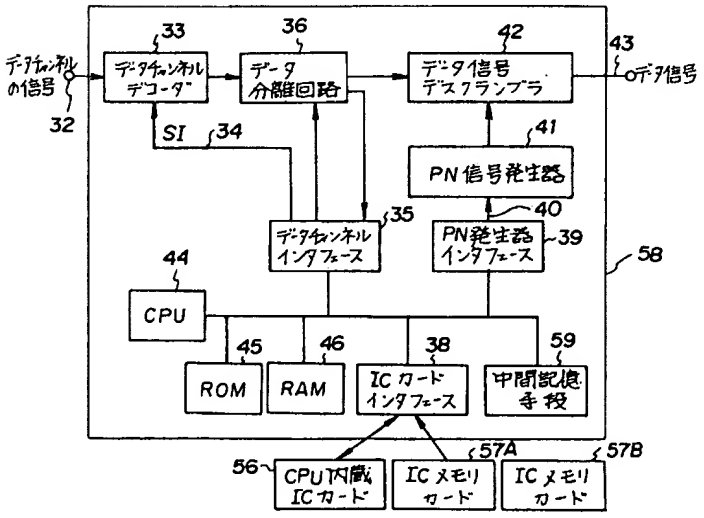
本発明による受信機構成の第1の実施例を示す図

第 1 図



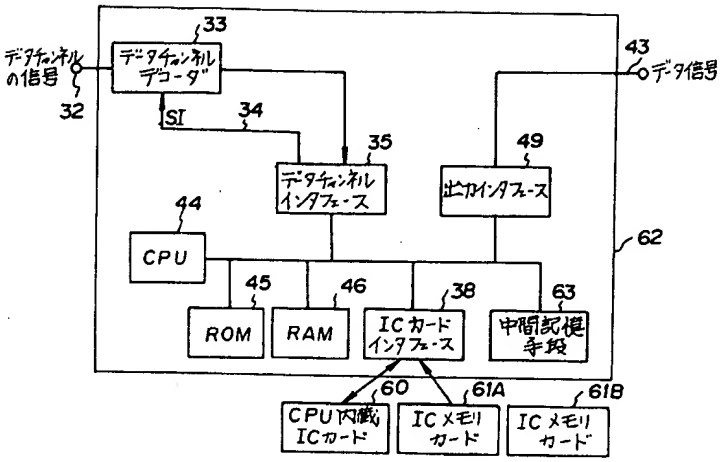
本発明による受信機構成の第2の実施例を示す図

第 2 図



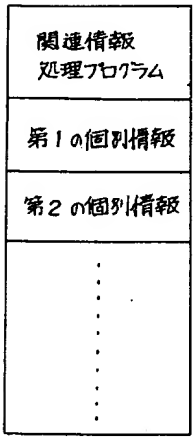
本発明をデータ放送の有料方式に適用した場合の
受信機構成の実施例(1)を示す図

第 3 図



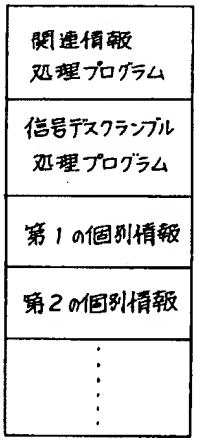
本発明をデータ放送の有料方式に適用した場合の受信機構成の実施例(2)を示す図

第 4 図



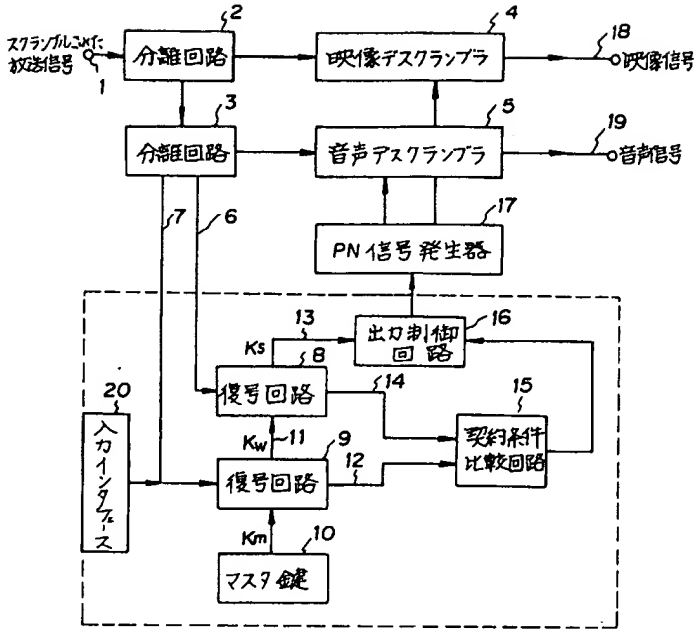
CPU内蔵のICカードに記録されている情報の例(信号デスクランブルをICカードの外部で行う場合)を示す図

第 5 図



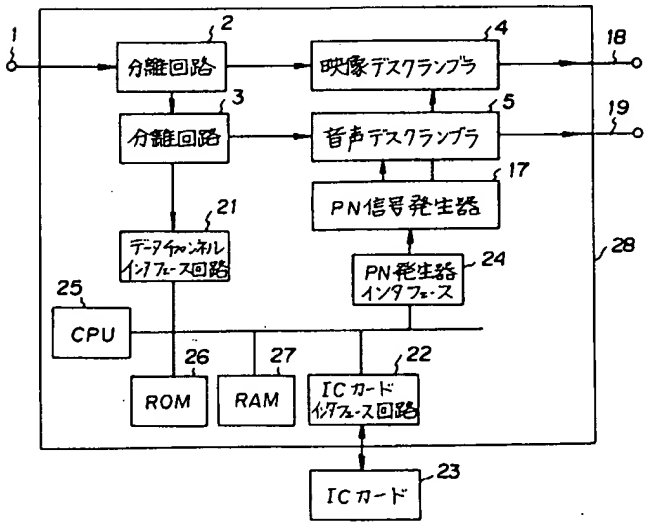
CPU内蔵のICカードに記録されている情報の例(信号デスクランブルをICカードの内部で行う場合)を示す図

第 6 図



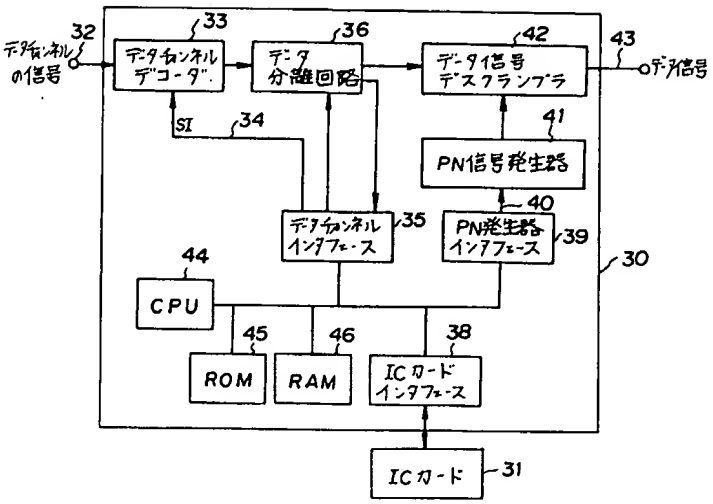
従来のテレビジョンやハイビジョンの有料放送受信機の機能ブロックの構成例を示す図

第 7 図



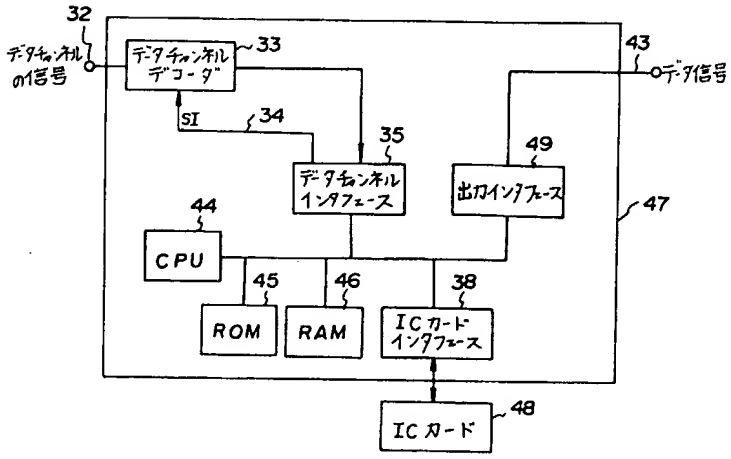
CPU内蔵のICカードを用いる有料放送受信機の回路構成例を示す図

第 8 図



データ放送の有料方式受信機の構成例(1)[デスクランブル処理を有料デコーダ本体内で行う場合]を示す図

第 9 図



データ放送の有料方式受信機の構成例(2)[デスクランブル処理をICカード内で行う場合]を示す図

第 10 図